UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/933,972	08/20/2001	Philip Hawkes	010497	7964

23696 7590 06/19/2009

QUALCOMM INCORPORATED
5775 MOREHOUSE DR.
SAN DIEGO, CA 92121

EXAMINER	
SIMITOSKI, MICHAEL J	
ART UNIT	PAPER NUMBER
2439	

NOTIFICATION DATE	DELIVERY MODE
06/19/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

us-docketing@qualcomm.com
kascanla@qualcomm.com
nanm@qualcomm.com

Office Action Summary	Application No.	Applicant(s)	
	09/933,972	HAWKES ET AL.	
	Examiner	Art Unit	
	MICHAEL J. SIMITOSKI	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 May 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 August 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *3/13/09*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The response of 5/28/2009 was received and considered.

2. The IDS of 3/13/09 was received and considered.

3. Claims 1-36 are pending.

Continued Examination Under 37 CFR 1.114

4. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 5/28/09 has been entered.

Response to Arguments

5. Applicant's arguments with respect to claims 1-36 have been considered but are moot in view of the new ground(s) of rejection. However, arguments that are believed applicable to the following action will be discussed below.

6. Applicant's response (p. 9) submits that the current claims are enabled based on the cited portion of the specification. For clarity, the portions of the specification are cited here:

> [1068] The following paragraph discusses how the SK is updated following a successful subscription process. Within each period for updating the BAK, a short-term interval is provided during which SK is distributed on a broadcast channel. The CS uses a cryptographic function to determine two values SK and SKI (SK Information) such that SK can be determined from BAK and SKI. For example, SKI may be the encryption of SK using BAK as the key. In the exemplary embodiment, SKI is an IPSec packet containing SK that is encrypted using BAK as the key. Alternatively, SK may be the result of applying a cryptographic hash function to the concatenation of the blocks SKI and BAK.
>
> [1069] Some portion of SKI may be predictable. For example, a portion of SKI may be derived from the system time during which this SKI is valid. This portion, denoted $SKI_{13}A$, need not be transmitted to the MS 300 as part of the broadcast service. The remainder of SKI, SKI_B may be unpredictable. The SKI_B need not be transmitted to the MS 300 as part of the broadcast service. The MS 300 reconstructs SKI from SKI_A and SKI_B and provides SKI to UIM 308. The SKI may be reconstructed within the UIM 308. The value of SKI must change for each new SK. Thus, either SKI_A and/or SKI_B must change when computing a new SK. The CS sends SKI_B to BS for broadcast transmission. The BS broadcasts SKI_B,

> which is detected by the antenna 302 and passed to the receive circuitry 304. Receive circuitry 304 provides SKI_B to the MS 300, wherein the MS 300 reconstructs SKI. The MS 300 provides SKI to UIM 308, wherein the UIM 308 obtains the SK using the BAK stored in SUMU 314. The SK is then provided by UIM 308 to ME 306. The ME 306 stores the SK in memory storage unit, MEM 310. The ME 306 uses the SK to decrypt broadcast transmissions received from the CS.
>
> [1085] The SK is treated in a similar manner to RK. First SKI is derived from the SKI_A and SKI_B (SKI_B is the information transmitted from CS to MS). Then a predetermined function labeled d3 is used to derive the SK from SKI and BAK (stored in the SUMU 314), according to:
>
> [1086] SK=d3(BAK, SKI). (6)
>
> [1087] In one embodiment, the function d3 defines a cryptographic-type function. In an exemplary embodiment, SK is computed as:
>
> [1088] SK=SHA(BAK || SKI), (7)
>
> [1089] while in another embodiment, SK is computed as
>
> [1090] SK=AES(BAK, SKI). (8)

7. The specification describes multiple embodiments regarding the generation/updating of the second key (described in the specification as SK). The embodiment that most closely resembles the claimed invention is described in the above cited portions of the specification. Applicant cited ¶1068's " Alternatively, SK may be the result of applying a cryptographic hash function to the concatenation of the blocks SKI and BAK" in support of the instant amendment. However, the amendment recites:

> "updating the second key after a second time period has elapsed, wherein the second key is updated in two parts, a first part known to the participant in the transmission and a second part sent on the broadcast channel, and wherein the first part and the second part are concatenated to determine the second key using a cryptographic function." (claim 1, last limitation)

However, the specification does not describe determining the second key (SK) by concatenating a first part known to the participant in the transmission and a second part *sent on the broadcast channel*. In this embodiment of the specification, the SKI (claimed second part that is concatenated with BAK, see ¶1068, cited in applicant's response, and ¶1088) is not sent over the broadcast channel. Rather, the SKI also comprises two parts, SKI_A and SKI_B where, SKI_B is sent over the broadcast channel (¶1069). As such, the specification does not provide support for the instant claims.

8. Addressing the art, the claims being best understood, the previously-applied prior art has been discussed. Further, the newly-cited reference to IEEE teaches WEP, a well known protocol for communicating privately. WEP operates where each end of a secure communication has the secret key (first part known to a participant, p. 64, ¶1), where the secret key is combined with an initialization vector (IV) that is received over a broadcast channel (second part sent on a broadcast channel, p. 64, ¶3) where the IV and secret key are concatenated to determine a content-encrypting key (key sequence) using a cryptographic function (pseudo-random number generator, Fig. 44). This method provides benefits such as that the IV can be sent in the clear and since the IV travels with the message, the receiver can always decipher the message (p. 64, ¶3). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Richards such that the last key, SK generated from an initialization vector received with the content and PK (equivalent to the WEP secret key). In this combination, PK is known to the recipient and an IV is received over the broadcast channel, where they are concatenated and applied to a cryptographic function to generate the SK.

Claim Rejections - 35 USC § 112

9. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

10. Claims 1-36 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The specification does not describe receiving data over a broadcast channel, concatenating that data with other data and applying a cryptographic function to the concatenation to determine a key (see response above for more detail).

Claim Rejections - 35 USC § 101

11. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

12. Claims 1-13 & 27-30 are rejected under 35 U.S.C. 101 as not falling within one of the four statutory categories of invention. While the claims recite a series of steps or acts to be performed, a statutory "process" under 35 U.S.C. 101 must (1) be tied to particular machine, or (2) transform underlying subject matter (such as an article or material) to a different state or thing. See page 10 of In Re Bilski 88 USPQ2d 1385. The instant claims are neither positively tied to a particular machine that accomplishes the claimed method steps nor transform underlying subject matter, and therefore do not qualify as a statutory process. The method including steps of determining, encrypting, sending and updating is broad enough that the claim could be completely performed mentally, verbally or without a machine nor is any transformation apparent.

13. Claims 22-23 & 33-36 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claims recite systems with "means", however, the specification describes that the various algorithms and steps could be performed using software alone (pre-grant publication, ¶106, ¶108). Therefore, the invention claimed does not fall within one of the statutory classes of invention defined under 35 U.S.C. §101.

14. Claims 24-26 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claims recite a digital storage device, however the device has no structural limitations except that it comprises code “for” performing steps. As the code or storage device is not utilized to perform or to cause a device to perform any steps, the code represents non-functional descriptive material. As such, the invention claimed does not fall within one of the statutory classes of invention defined under 35 U.S.C. §101.

Claim Rejections - 35 USC § 112

15. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

16. Claim 24-26 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

a. Regarding claims 24-26, the claims are directed to a digital storage device, however, the storage device comprises only instructions and therefore it is whether the claim is directed to a physical device or only software.

Claim Rejections - 35 USC § 103

17. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

18. Claims 1-5, 10-11, 13, 15-16 & 18-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6,690,795 to **Richards**, in view of "IEEE 802.11, Part 11 : Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications" by **IEEE**.

Regarding claims 1-5, 11, 13 & 22-24, Richards discloses determining a registration key (UEV) specific to a participant (set top box) in a transmission (Fig. 26, #130 & col. 20, lines 61-67), determining a first key (CCK_1, Fig. 26, #133), encrypting the first key (CCK_1) with the registration key (Fig. 26, #133), sending the encrypted first key ([CCK_1]UEV) to the participant in the transmission (set top box, Fig. 26, #133), determining a second key (SK) for decrypting content on a broadcast channel (Fig. 26,

#159), updating the first key (CCK) after a first time period has elapsed (Fig. 23) and updating the second key (SK) after a second time period has elapsed. Richards lacks updating the second key after a second time period has elapsed, wherein the second key is updated in two parts, a first part known to the participant in the transmission and a second part sent on the broadcast channel, and wherein the first part and the second part are concatenated to determine the second key using a cryptographic function. However, IEEE teaches WEP, a well known protocol for communicating privately. WEP operates where each end of a secure communication has the secret key (first part known to a participant, p. 64, ¶1), where the secret key is combined with an initialization vector (IV) that is received over a broadcast channel (second part sent on a broadcast channel, p. 64, ¶3) where the IV and secret key are concatenated to determine a content-encrypting key (key sequence) using a cryptographic function (pseudo-random number generator, Fig. 44). This method provides benefits such as that the IV can be sent in the clear and since the IV travels with the message, the receiver can always decipher the message (p. 64, ¶3). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Richards such that the last key, SK generated from an initialization vector received with the content and PK (equivalent to the WEP secret key), such that PK is known to the recipient and an IV is received over the broadcast channel, where they are concatenated and applied to a cryptographic function to generate the SK. One of ordinary skill in the art would have been motivated to perform such a modification to gain benefits such as that the IV can be sent in the clear and since the IV travels with the message, the receiver can always decipher the message (p. 64, ¶3).

Regarding claim 10, Richards discloses transmitting the encrypted first key ([CCK_1]UEV, col. 9, line 58 – col. 10, line 5).

Regarding claims 15 & 16, Richards discloses in a wireless system (col. 20, lines 61-67) receiver circuitry (set top box) adapted to perform receiving a registration key (UEV) specific to a participant (set top box) in a transmission (Fig. 26, #130), determining a first key (CCK_1, Fig. 26, #133), encrypting the

first key (CCK_1) with the registration key (Fig. 26, #133), sending the encrypted first key ([CCK_1]UEV) to the participant in the transmission (set top box, Fig. 26, #133), determining a short-time key (SK), updating the first key (CCK) after a first time period has elapsed (Fig. 23) and updating the short-time key (SK) after a second time period has elapsed, a user identification unit (set-top box, col. 4, lines 55-62), operative to determine a short-time key (SK) for decrypting a broadcast message (content, col. 9, lines 11-33), comprising a processing unit (decryption hardware) to decrypt key information (col. 9, lines 11-33) and a mobile equipment unit (decryption hardware) adapted to apply the short-time key for decrypting the broadcast message (content, col. 4, lines 55-62 & col. 9, lines 11-33), but lacks wherein the short-time key is updated in two parts wherein the first part and the second part are concatenated to determine the short-time key using a cryptographic function. However, IEEE teaches WEP, a well known protocol for communicating privately. WEP operates where each end of a secure communication has the secret key (first part known to a participant, p. 64, ¶1), where the secret key is combined with an initialization vector (IV) that is received over a broadcast channel (second part sent on a broadcast channel, p. 64, ¶3) where the IV and secret key are concatenated to determine a content-encrypting key (key sequence) using a cryptographic function (pseudo-random number generator, Fig. 44). This method provides benefits such as that the IV can be sent in the clear and since the IV travels with the message, the receiver can always decipher the message (p. 64, ¶3). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Richards such that the last key, SK generated from an initialization vector received with the content and PK (equivalent to the WEP secret key), such that PK is known to the recipient and an IV is received over the broadcast channel, where they are concatenated and applied to a cryptographic function to generate the SK. One of ordinary skill in the art would have been motivated to perform such a modification to gain benefits such as that the IV can be sent in the clear and since the IV travels with the message, the receiver can always decipher the message (p. 64, ¶3).

Regarding claim 18, Richards, as modified, discloses the memory storage unit storing a broadcast access key (IEEE's secret key, p. 64) and wherein the processing unit determines the short-time key (Richard's SK, as modified, IEEE's key sequence) using the broadcast access key (secret key, p. 64).

Regarding claim 19, Richards discloses the short-time key (SK) being updated at a first frequency (col. 9, lines 32-36 & Fig. 16).

Regarding claim 20, Richards discloses the broadcast access key (PK) being updated at a second frequency less than the first frequency (Figs. 9 & 10).

Regarding claim 21, Richards discloses a video service (col. 2, lines 39-55).

19. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Richards** and **IEEE**, as applied to claim 4 above, in further view of "FOLDOC, Free On-Line Dictionary Of Computing" by **LinuxGuruz**. Richards discloses using the system for distributing information on computer networks, but lacks specifically Internet Protocol packets. However, LinuxGuruz teaches that Internet Protocol packets are widely used on Ethernet networks for packet routing (§Internet Protocol). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to broadcast Internet Protocol packets. One of ordinary skill in the art would have been motivated to perform such a modification because Internet Protocol packets are used on Ethernet networks, as taught by LinuxGuruz (§Internet Protocol).

20. Claims 7-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Richards** and **IEEE**, as applied to claim 3 above, in further view of Applied Cryptography, Second Edition by **Schneier**.

Regarding claim 7, Richards lacks calculating a registration key information message and transmitting the registration key information message. However, Schneier teaches that no encryption key should be used for an indefinite period (p. 183, §8.10) and should be replaced (p. 184, ¶3). Therefore, it

would have been obvious to one having ordinary skill in the art at the time the invention was made to update the registration key and hence calculate a registration key information message and transmit the registration key information message. One of ordinary skill in the art would have been motivated to perform such a modification to update the registration key, as taught by Schneier (pp. 183-184).

Regarding claim 8, Richards discloses calculating a first key (CCK_1) information message (new encrypted key) and transmitting the first key information message (col. 10, lines 1-5).

Regarding claim 9, Richards discloses calculating a second key (SK (IV, as modified by IEEE)) information message (new encrypted key) and transmitting the second key information message (col. 9, lines 58-62).

21. Claims 12 & 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Richards** and **IEEE**, as applied to claims 11 & 15 above, in further view of U.S. Patent 6,073,122 to **Wool**. Richards discloses storing the second key (SK) in a memory storage unit (col. 5, lines 60-63), but lacks the first key stored in secure memory storage unit. However, Wool teaches that set-top boxes often contain secure memory to minimize piracy of encryption keys stored (col. 1, lines 44-52). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to store the first key in a secure memory storage unit. One of ordinary skill in the art would have been motivated to perform such a modification to minimize piracy of encryption keys stored, as taught by Wool (col. 1, lines 44-52).

22. Claims 25, 27, 29, 31, 33 & 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Richards** and **IEEE**, as applied to claims 24, 1, 11, 15, 22 & 23, respectively, in further view of U.S. Patent 6,536,041 to Knudson et al. (**Knudson**).

Regarding claims 25, 27, 29, 31, 33 & 35, Richards, as modified, lacks the first part including a time value. However, Knudson teaches that a unique key for an event can include a concatenation of a

start time and date for the event (video event, col. 11, line 55 – col. 12, line 4) to create a key for the real-time event (col. 12, lines 21-27). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Richards, as modified above, such that the first part includes a time value. One of ordinary skill in the art would have been motivated to perform such a modification to generate a key for a real-time event, as taught by Knudson.

23. Claims 26, 28, 30, 32, 34 & 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Richards** and **IEEE**, as applied to claims 24, 1, 11, 15, 22 & 23, respectively, in further view of U.S. Patent 5,778,069 to Thomlinson et al. (**Thomlinson**).

Regarding claims 26, 28, 30, 32, 34 & 36, Richards, as modified, lacks wherein the second key is determined by applying a cryptographic hash function to the concatenation of the first and second parts. However, Thomlinson teaches a pseudo-random number generator (col. 3, lines 29-33) that takes as its input, a hash (col. 3, lines 41-45) of concatenated values (col. 5, lines 56-61), gaining the benefit of preventing observable biasing (reduces the likelihood of a breach of the seed, col. 6, lines 2-10). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Richards, as modified above, to hash the concatenation of the inputs before inputting them into the pseudo random number generator (IEEE). One of ordinary skill in the art would have been motivated to perform such a modification to prevent observable biasing, as taught by Thomlinson.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL J. SIMITOSKI whose telephone number is (571)272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on (571)272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

June 12, 2009
/Michael J Simitoski/
Primary Examiner, Art Unit 2439